(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 27 722 A 1**

(51) Int. Cl.[6]: **B 60 R 25/00**
G 08 C 17/02
E 05 B 49/00
// E05B 65/36

(21) Aktenzeichen: 198 27 722.9
(22) Anmeldetag: 22. 6. 98
(43) Offenlegungstag: 23. 12. 99

USSN: 09/743,632
A.U.: 2631

(71) Anmelder:
Bayerische Motoren Werke AG, 80809 München, DE

(72) Erfinder:
Bartz, Rüdiger, 80809 München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	196 42 017 C1
DE	196 05 836 C1
DE	197 36 302 A1
DE	43 18 596 A1
DE	39 27 024 A1
DE	32 44 566 A1
GB	23 00 739 A
GB	22 89 358 A

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Sicherheitseinrichtung

(57) Bei einer Sicherheitseinrichtung für Fahrzeuge ist vom Fahrzeug ein Fragecodesignal und von einem tragbaren Transponder ein Antwortcodesignal aussendbar und im Fahrzeug verarbeitbar. Das Antwortcodesignal weist eine überlagerte eindeutige Kennung auf, deren Existenz Voraussetzung für die Verarbeitung des Antwortcodesignals ist.

DE 198 27 722 A 1

Beschreibung

Die Erfindung bezieht sich auf eine Sicherheitseinrichtung mit den Merkmalen des Oberbegriffs von Patentanspruch 1.

Eine derartige Sicherheitseinrichtung ist aus der DE 40 03 280 A bekannt. Dabei wird die Benutzung des Fahrzeugs durch einen Unberechtigten verhindert, indem entweder das Frage- oder das Antwort-Codesignal nur über eine kurze Reichweite verfügt und daher nur dann wirksam wird, wenn sich der Benutzer in unmittelbarer Nähe des Fahrzeugs befindet. In der Zwischenzeit sind Voll-Duplex-Transceiver bekannt, die es ermöglichen, die bekannte Sicherheitseinrichtung zu "überlisten". Befindet sich ein derartiger Transceiver in unmittelbarer Nähe des Fahrzeugs und ein weiterer Transceiver in der Mähe des berechtigten Benutzers, wird über die beiden Transceiver eine künstliche Verlängerung der Reichweite erzielt. Für das Fahrzeug bzw. für den berechtigten Benutzer, die das Codesignal mit kleiner Reichweite aussenden, wird dieses Codesignal durch den nächstliegenden Transceiver aufgenommen und zum anderen Transceiver weitergeleitet. Dadurch ist eine Manipulation möglich, auch wenn sich der berechtigte Benutzer in großer Entfernung vom Fahrzeug befindet. Sie ist sogar dann möglich, wenn seine Entfernung größer als die Reichweite des Codesignals mit der großen Reichweite ist. Voraussetzung hierfür ist lediglich, daß die Übertragungsstrecke der beiden Transceiver entsprechend groß ist.

Der Erfindung liegt die Aufgabe zugrunde, eine Sicherheitseinrichtung der eingangs genannten Art zu schaffen, mit der ein wirksamer Schutz der Sicherheitseinrichtung vor einer bewußten Reichweitenverlängerung erzielt wird.

Die Erfindung löst diese Aufgabe durch die Merkmale des Patentanspruchs 1.

Durch die Kennung des Antwort-Codesignals wird diesem eine zusätzliche Charakteristik mitgegeben. Nur dann, wenn diese Kennung des Antwort-Codesignals der im Empfänger erwarteten Kennung entspricht, wird das Antwort-Codesignal wirksam und führt ggf. zu der gewünschten Funktion des Fahrzeugs, d. h. im Falle einer Zugangskontrolle z. B. zum Öffnen des Fahrzeugs.

Diese Kennung kann auf unterschiedliche Weise gestaltet sein. Besonders vorteilhaft ist sie dann, wenn es sich dabei um keine vorgegebene und vorhersehbare Kennung, sondern um eine Kennung handelt, die nach Außen hin zufällig erscheint. Ist die Kennung insbesondere vom Dateninhalt des Antwort-Codesignals abhängig, so kann zwar der Empfänger ohne weiteres die Kennung mit dem Dateninhalt des Antwort-Codesignals in Beziehung setzen und ggf. den autorisierten Benutzer identifizieren.

Ein einfacher Transceiver hingegen ist nicht in der Lage, die Kennung zeitgleich (d. h. ohne Zeitverlust gegenüber einem nicht mit einer derartigen Kennung versehenen Codesignal) weiterzugeben, da er zunächst die Datenbits hinsichtlich der Kennung untersuchen muß und diese Kennung zusammen mit den Datenbits an den anderen Transceiver übertragen muß. Dort ist es wiederum erforderlich, erneut diese Kennung den Datenbits aufzuprägen und an das Fahrzeug weiterzugeben. Es ist ohne weiteres zu erkennen, daß die zweimalige Analyse bzw. Umsetzung der Kennung der einzelnen Datenbits in den jeweiligen Transceivern zeitaufwendig ist und zu einer Laufzeiterhöhung des empfangenen Signals führt.

Wird nun im Empfänger die Laufzeit des Antwort-Codesignals so bemessen, daß sie gleich der Laufzeit von Frage- und Antwort-Codesignal bei einem im Nahbereich befindlichen berechtigten Fahrzeugbenutzer ist, läßt sich dadurch eine Laufzeitbegrenzung für das Antwort-Codesignal die

Reichweitenmanipulation erkennen und das ggf. bei einer derartigen tatsächlichen oder durch die o. g. beschriebene, scheinbare Verlängerung der Laufstrecke sich ergebende, verzögert eingehende Antwort-Codesignal nicht wirksam werden.

Weitere Verbesserungen der Erfindung beschäftigen sich mit Einzelmaßnahmen zur Anwendung der Kennung und zielen ebenfalls darauf ab, die Laufzeit des im Fahrzeug eingehenden Signals zu erhöhen. Sie sind Gegenstand der Patentansprüche 3 bis 6 und werden anhand der Zeichnung weiter erläutert.

In der Zeichnung ist ein Ausführungsbeispiel der Erfindung dargestellt. Es zeigt

Fig. 1 den grundsätzlichen Aufbau eines mobilen Transponders, der im Rahmen der Erfindung Verwendung findet und

Fig. 2 ein Beispiel für ein Antwort-Codesignal, das sich unter Verwendung des Transponders ergibt.

Der in **Fig.** 1 dargestellte Transponder enthält einen HF-Empfänger **1** sowie einen HF-Sender **2**, die über Antennen **3** und **4** mit einem Fahrzeug (nicht dargestellt) in einer Funkverbindung stehen. Der Empfänger **1** nimmt ein Frage-Codesignal ("Challenge") auf, das vom Fahrzeug ausgesandt wird und das in **Fig.** 2 beispielshaft dargestellt ist.

Der mit ID-Geber bezeichnete Transponder liefert ein Antwort-Codesignal ("Response (intern))" genannt und in **Fig.** 2 wiederum beispielshaft gezeigt), das beispielsweise aus dem Challenge-Code unter Zugrundeliegen eines definierten Algorithmus gebildet wird. Der Algorithmus ist einem Speicher **5** enthalten und mit "geheimer Code" bezeichnet und in **Fig.** 2 exemplarisch gezeigt. Die Berechnung des Antwort-Codesignals erfolgt in einer Logikeinheit **6**, die mit Kryptoberechnung bezeichnet ist. Die Logikeinheit **6** liefert das Antwort-Codesignal, das als Bitmuster 0, 1, vorliegt und beispielsweise eine Länge von mehreren Bytes besitzt. Dieses Bitmuster stellt einen mit Daten bezeichneten Dateninhalt dar, der an den Sender **2** weitergegeben wird.

Erfindungsgemäß wird zusätzlich eine als Sendeleistungsmaske bezeichnete Kennung erzeugt, die abhängt einerseits von dem für die Berechnung des Antwort-Codesignals maßgeblichen Algorithmus (Geheimer Code) und dem Dateninhalt des Antwort-Codesignals selbst. Diese Kennung wird in einer Logikeinheit **7** ("Maskenberechnung") berechnet und als Sendeleistungsmaske ebenfalls an den Sender **2** weitergegeben.

Die Sendeleistungsmaske veranlaßt den Sender **2** dazu, das Antwort-Codesignal in der Weise auszugeben, daß bestimmte Bits des Antwort-Codesignals mit einer reduzierten Sendeleistung von z. B. 50% des Maximums übertragen werden. Das vom Sender **2** übertragene Antwortsignal ("Response (extern)" genannt) ist in **Fig.** 2 beispielhaft gezeigt.

Der Empfänger nimmt das Antwort-Codesignal auf und wertet es zunächst hinsichtlich seines Dateninhalts aus. Da der zugrundeliegende Algorithmus im Empfänger ebenfalls bekannt ist, kann der Empfänger analog der Logikeinheit **7** die Sendeleistungsmaske berechnen und dem empfangenen Antwort-Codesignal überlagern. Da der berechtigte Benutzer bei einem korrekten Ablauf sich im Nahbereich des Fahrzeugs befindet, ist diese durch die Sendeleistungsmaske gegebene Zusatzinformation im Empfänger des Fahrzeugs auch auswertbar und, da das Antwort-Codesignal zeitkorrekt vorliegt, hinsichtlich der Richtigkeit der aufgeprägten Sendeleistungsmaske identifzierbar. Bei korrektem Ablauf erkennt das Fahrzeug daher den berechtigten Benutzer anhand der Übereinstimmung des Dateninhalts und der Sendeleistungsmaske des (externen) Antwort-Codesignals.

Wird, wie eingangs geschildert, mit zwei Transceivern gearbeitet, ergibt sich bedingt durch das notwendige Erken-

nen der Sendeleistungen jedes einzelnen Bits eine Zeitverzögerung in der Weitergabe der einzelnen Bits des externen Antwort-Codesignals von dem ersten Transceiver zum zweiten Transceiver und zusätzlich vom zweiten Transceiver zum Fahrzeug.

Wird der Zeitpunkt, zu dem das Antwort-Codesignal im Fahrzeug eingeht, kleiner als eine Bitzeit festgelegt, bietet das erfindungsgemäße Verfahren auch gegen einen "intelligenten" Transceiver wirkungsvollen Schutz, da dieser zunächst ein Bit zur Bestimmung der Sendefeldstärke einlesen muß und diese zusätzliche Information codiert an den zweiten Transceiver übertragen muß. Aufgrund der Distanz der beiden Transceiver zueinander muß die zusätzliche Information vom ersten Transceiver separat übertragen werden und am zweiten Transceiver entsprechend umgesetzt werden, was nicht ohne Zeitverlust möglich ist. Das derart übertragene Antwort-Codesignal gelangt deutlich verspätet zum Fahrzeug und kann aufgrund dieser Zeitverzögerung als nicht vom autorisierten Benutzer stammend erkannt werden.

Dadurch ist es auch unwirksam, auch wenn der Dateninhalt und auch die Sendeleistungsmaske die erwarteten Eigenschaften besitzen. Besitzt es keine Kennung oder aber eine nicht mit der erwarteten übereinstimmende Kennung, bleibt es selbstverständlich ebenfalls unwirksam. Damit ergibt sich eine deutliche Verbesserung von Sicherheits-Einrichtungen und insbesondere schlüssellosen Zugangssystemen, da diese auch gegenüber einer Reichweitenmanipulation geschützt sind. Zusätzliche Maßnahmen, wie aus der eingangs genannte DE 40 03 280 A bekannt und darin bestehend, die Sendeleistung der beiden Codesignale unterschiedlich zu gestalten können dann ebenfalls wegfallen.

Patentansprüche

1. Sicherheits-Einrichtung für Fahrzeuge, bei der vom Fahrzeug ein Fragecodesignal und von einem tragbaren Transponder ein Antwortcodesignal aussendbar und im Fahrzeug verarbeitbar ist, **dadurch gekennzeichnet**, daß das Antwortcodesignal eine überlagerte, eindeutige Kennung aufweist, deren Existenz Voraussetzung für die Verarbeitung des Antwortcodesignals ist.
2. Einrichtung nach Anspruch 1, dadurch gekennzeichnet, daß die Kennung vom Dateninhalt des Antwortcodesignals abhängt.
3. Einrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Kennung eine Markierung der Datenbits ist.
4. Einrichtung nach Anspruch 3, dadurch gekennzeichnet, daß die Markierung für Datenbits gleichen Informationsgehalts unterschiedlich ist.
5. Einrichtung nach Anspruch 3 oder 4, dadurch gekennzeichnet, daß die Markierung in einer Variation der Sendeleistung der Datenbits besteht.
6. Einrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Bitzeit größer der zeitliche Abstand zwischen der Abgabe des Fragecodesignals und der Eingangszeit des Antwortcodesignals ist.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 198 27 722 A1
Int. Cl.[6]: B 60 R 25/00
Offenlegungstag: 23. Dezember 1999

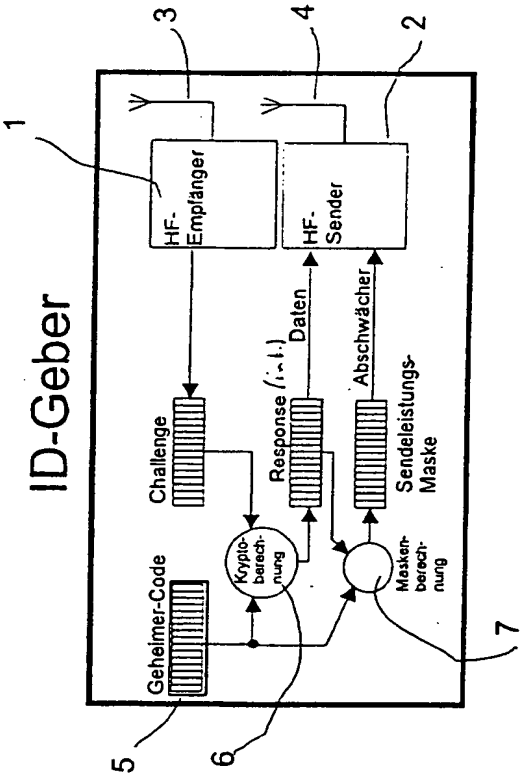
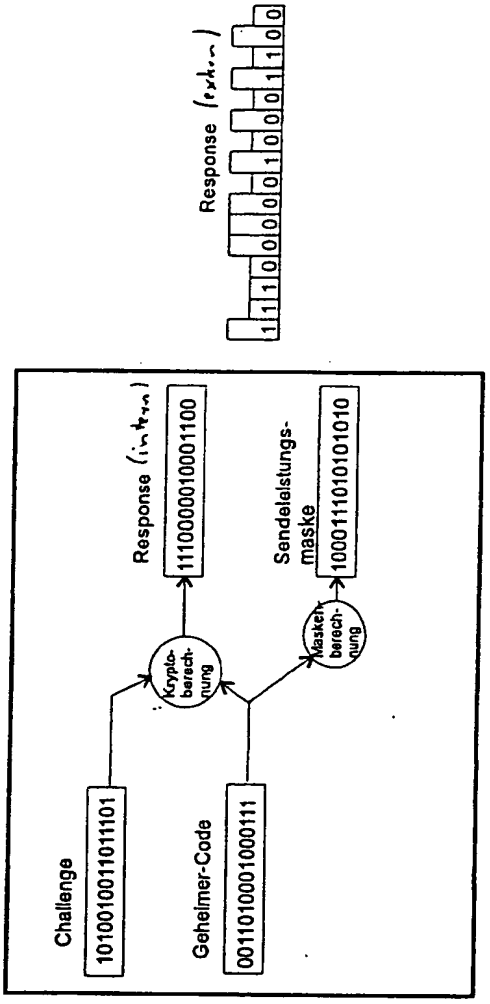


Fig. 1



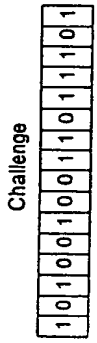


Fig. 2